Grover's search with faults on some marked elements

Dmitry Kravchenko, Nikolajs Nahimovs, Alexander Rivosh[*]

Faculty of Computing, University of Latvia

Abstract. Grover's algorithm is a quantum query algorithm solving the unstructured search problem of size N using $O(\sqrt{N})$ queries. It provides a significant speed-up over any classical algorithm [Gro96].

The running time of the algorithm, however, is very sensitive to errors in queries. It is known that if query may fail (report all marked elements as unmarked) the algorithm needs $\Omega(N)$ queries to find a marked element [RS08]. [AB+13] have proved the same result for the model where each marked element has its own probability to be reported as unmarked.

We study the behavior of Grover's algorithm in the model where the search space contains both faulty and non-faulty marked elements. We show that in this setting it is indeed possible to find one of non-faulty marked items in $O(\sqrt{N})$ queries.

We also analyze the limiting behavior of the algorithm for a large number of steps and show the existence and the structure of limiting state ρ_{lim}.

1 Introduction

Grover's algorithm is a quantum query algorithm solving the unstructured search problem of size N using $O(\sqrt{N})$ queries. It is known that any deterministic or randomized algorithm needs linear time (number of queries) to solve the above problem. Thus, Grover's algorithm provides a significant speed-up over any classical algorithm.

The running time of the algorithm (number of queries), however, is very sensitive to errors in queries. Regev and Schiff [RS08] have shown that if query has a small probability of failing (reporting that *none* of the elements are marked), then quantum speed-up disappears: no quantum algorithm can be faster than a classical exhaustive search by more than a constant factor. Ambainis et al. [AB+13] have studied Grover's algorithm in the model where each marked element has its own probability to be reported as unmarked, independent of probabilities of other marked elements. Similarly to the result of [RS08], they have shown that if all marked elements are faulty (have non-zero probability of failure) then the algorithm needs $\Omega(N)$ queries to find a marked element.

Although, technically the model of [AB+13] allows one non-faulty marked element[1] (element with zero probability of failure) this case was not included into the analysis.

We study the behavior of the algorithm in the model where the search space contains both faulty and non-faulty marked items. Specifically, we focus on the case where the search space contains multiple non-faulty and one faulty marked element. We analyze the effect of a fault on the state of the algorithm and show that in this setting it is indeed possible to find one of non-faulty marked elements in $O(\sqrt{N})$ queries. Up to the best our knowledge, this is the first demonstrggggation of query fault modes which can be tolerated by the Grover's algorithm.

We also analyze the limiting behavior of Grover's algorithm for a large number of steps and show the existence and the structure of limiting state ρ_{lim}. The limiting state is a mixture of a faulty marked element $|i\rangle$ with probability $\frac{1}{3}$, the uniform superposition of all non-faulty marked elements with probability $\frac{1}{3}$ and the uniform superposition of all non-marked elements with probability $\frac{1}{3}$. Using the approach of [AB+13] one can show that convergence time is $O(N)$.

The contrast between this result and the algorithm finding a marked element in $O(\sqrt{N})$ steps can be explained by the probability of finding a marked element oscillating between $\Omega(1)$ and $o(1)$ until these oscillations finally die off after $O(N)$ steps.

2 Technical preliminaries

We use the standard notions of quantum states, density matrices etc., as described in [KLM07].

Grover's algorithm [Gro96]

Suppose we have an unstructured search space of size N. Grover's algorithm starts with a starting state $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle$. Each step of the algorithm consists of two transformations: Q and D. Here, Q is a query to a black box defined by

- $Q|i\rangle = -|i\rangle$ if i is a marked element;
- $Q|i\rangle = |i\rangle$ if i is not a marked element.

D is the diffusion transformation described by the following $N \times N$ matrix:

$$
D = \begin{pmatrix}
-1 + \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\
\frac{2}{N} & -1 + \frac{2}{N} & \cdots & \frac{2}{N} \\
\cdots & \cdots & \cdots & \cdots \\
\frac{2}{N} & \frac{2}{N} & \cdots & -1 + \frac{2}{N}
\end{pmatrix}.
$$

---

[1] The limitation of at most one non-faulty marked element comes from the probability independence assumption – two or more marked elements with zero error probability of failure would not be independent.

We refer to $|\psi_t\rangle = (DQ)^t|\psi_0\rangle$ as the state of Grover's algorithm after t time steps.

Grover's algorithm has been analyzed in detail and many facts about it are known [Amb04]. If there is one marked element i, the probability of finding it by measuring $|\psi_t\rangle$ reaches $1 - o(1)$ for $t = O(\sqrt{N})$. If there are k marked elements, the probability of finding one of them by measuring $|\psi_t\rangle$ reaches $1 - o(1)$ for $t = O(\sqrt{N/k})$.

Spherical trigonometry

Spherical trigonometry is a branch of geometry which deals with the relationships between trigonometric functions of the sides and angles of the spherical polygons. Trigonometry on a sphere differs from the traditional planar trigonometry. For example, all distances are measured as angular distances.

In the context of this paper we need only a few basic formula for right spherical triangles. Let ABC be a right spherical triangle with a right angle C. Then the following following set of rules (known as Napier's rules) applies:

$$\cos c = \cos a \cos b \quad \text{(R1)} \qquad \tan b = \cos A \tan c \quad \text{(R6)}$$
$$\sin a = \sin A \sin c \quad \text{(R2)} \qquad \tan a = \cos B \tan c \quad \text{(R7)}$$
$$\sin b = \sin B \sin c \quad \text{(R3)} \qquad \cos A = \sin B \cos a \quad \text{(R8)}$$
$$\tan a = \tan A \sin b \quad \text{(R4)} \qquad \cos B = \sin A \cos b \quad \text{(R9)}$$
$$\tan b = \tan B \sin a \quad \text{(R5)} \qquad \cos c = \cot A \cot B \quad \text{(R10)}$$
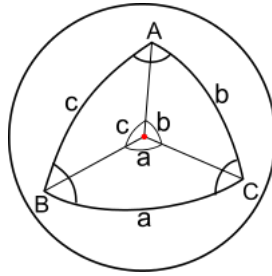

Fig. 1. Spherical trigonometry basic triangle.

For more detailed introduction into spherical trigonometry see [Tod86].

3 Model and results

Error model

Suppose we have a search space of size N containing k marked elements $i_1, i_2, \ldots, i_k$. First $k-1$ marked elements are *non-faulty* – the query always returns them as marked. Last marked element is *faulty* – the query might return it as unmarked.

More formally, on each step, instead of the correct query Q, we apply a faulty query Q' defined as follows:

- $Q'|i_k\rangle = |i_k\rangle$ with probability p;
- $Q'|i_k\rangle = -|i_k\rangle$ with probability $1-p$;
- $Q'|j\rangle = Q|j\rangle$ if $j \neq i_k$.

Summary of results

First we show that if there is at least one non-faulty marked element, then it is still possible to find a non-faulty marked element in $O(\sqrt{N})$ queries with $\Theta(1)$ probability.

Theorem 1 *Let $k \geq 3$, then we can choose $t = O(\sqrt{N/k})$ so that, if we run Grover's algorithm for t steps and measure the final state, the probability of finding a marked element is at least $\cos^2 \frac{\pi}{8} = 0.85\ldots$.*

For $k = 2$, the probability of finding a marked element is at least $\cos^2 \frac{\pi}{8} = 0.85\ldots$ under a promise that at most one fault occurs and at least $0.74\ldots$ in the general case.

We conjecture that, for $k = 2$, the probability is at least $0.85\ldots$ even in the general case.

Second, we analyze the limiting behavior of the algorithm for a large number of steps and show the existence and structure of limiting state ρ_{lim}.

Theorem 2 *Let ρ_t be the density matrix of state of Grover's algorithm with a faulty oracle Q' after t queries. Then, the sequence $\rho_1, \rho_2, \ldots$ converges to*

$$\rho_{lim} = \frac{1}{3}|\psi_+\rangle\langle\psi_+| + \frac{1}{3}|i_k\rangle\langle i_k| + \frac{1}{3}|\psi_-\rangle\langle\psi_-|$$

where $|\psi_+\rangle = \frac{1}{\sqrt{k-1}} \sum_{j=1}^{k-1} |i_j\rangle$ is the uniform superposition over all non-faulty marked elements and $|\psi_-\rangle = \frac{1}{\sqrt{N-k}} \sum_{i \neq i_j} |i\rangle$ is the uniform superposition over all non-marked elements.

4 Search

In this section we analyze the evolution of the state of Grover's algorithm in presence of multiple non-faulty and one faulty marked item. First we review the original Grover's algorithm, then we describe the effect of faults on the state of the algorithm. We derive upper bounds on the effect of faults and provide a modification of the original Grover's search algorithm which finds one of non-faulty marked items with $\Theta(1)$ probability in $O(\sqrt{N})$ queries.

4.1 No faulty marked items

Let us first consider the very basic search problem of Grover's algorithm. Namely, we have N items among which k are marked[2].

Operator D is symmetric w.r.t. permutations of amplitudes of all items, and operator Q is symmetric w.r.t. permutations of amplitudes of marked items, as well as permutations of amplitudes of non-marked items. So, on any step t amplitudes of all marked items are equal to each other and amplitudes of all non-marked items are equal to each other. Thus, we can represent $|\psi_t\rangle$ as:

$$|\psi_t\rangle = \sum_{i \in U} \alpha_t |i\rangle + \sum_{j \in M} \beta_t |j\rangle,$$

where U stands for the set of indexes of non-marked items and M stands for the set of indexes of k marked items. α_t and β_t denote the amplitudes of respectively a non-marked item and a marked item on step t. At each step of the algorithm we shall take care of two numbers only:

$$\alpha_t \sqrt{N-k} \qquad \text{and} \qquad \beta_t \sqrt{k}. \tag{1}$$

Since $|\psi_t\rangle$ is a unit vector, we have

$$\sum_{i \in U} \alpha_t^2 + \sum_{j \in M} \beta_t^2 = 1.$$

Thus, values (1) meet the equality $\left(\alpha_t \sqrt{N-k}\right)^2 + \left(\beta_t \sqrt{k}\right)^2 = 1$ and correspond to a point on the unit circle.

Initially all amplitudes are equal, so $\alpha = \beta = \frac{1}{\sqrt{N}}$, and the numbers (1) are

$$\alpha_0 \sqrt{N-k} = \frac{\sqrt{N-k}}{\sqrt{N}} \qquad \text{and} \qquad \beta_0 \sqrt{k} = \frac{\sqrt{k}}{\sqrt{N}}. \tag{2}$$

During the first step of the algorithm operator D does not change amplitudes of the state $|\psi_0\rangle$, and operator Q negates amplitudes of all marked items: $\beta_1 = -\beta_0 = -\frac{1}{\sqrt{N}}$. So the numbers (1) are

$$\alpha_1 \sqrt{N-k} = \frac{\sqrt{N-k}}{\sqrt{N}} \qquad \text{and} \qquad \beta_1 \sqrt{k} = -\frac{\sqrt{k}}{\sqrt{N}}. \tag{3}$$

According to (2) and (3), transformation $|\psi_0\rangle \xrightarrow{DQ} |\psi_1\rangle$ can be represented on the unit circle as shown on Figure 2. As before, we assume $k \ll N$, so that $\sqrt{k} \ll \sqrt{N-k}$, and the angle between $|\psi_0\rangle$ and $|\psi_1\rangle$ is

$$2 \arcsin\left(\frac{\sqrt{k}}{\sqrt{N}}\right) \approx 2\frac{\sqrt{k}}{\sqrt{N}} \tag{4}$$

---

[2] It is usually considered that $k \ll N$, as for $\frac{k}{N} \geq \lambda$ with sufficiently large λ the search problem can be trivially solved by a probabilistic algorithm in time $O\left(\lambda^{-1}\right)$.
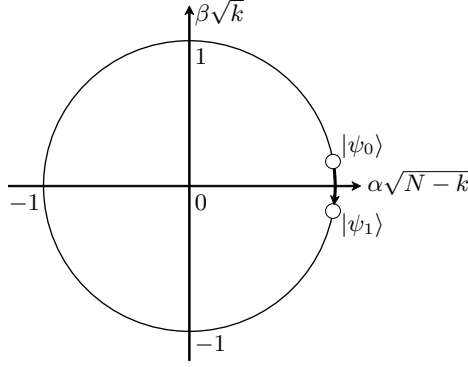
Fig. 2. The first step of Grover's algorithm

(this approximation holds for small-valued $\frac{\sqrt{k}}{\sqrt{N}}$).

Similarly, all further applications of operator DQ are nothing but clockwise rotations by angle $\sim 2\frac{\sqrt{k}}{\sqrt{N}}$. After $\sim \frac{\pi/2}{2\sqrt{k}/\sqrt{N}} = \frac{0.785...\sqrt{N}}{\sqrt{k}}$ such rotations the resulting state $|\psi_{\lfloor 0.785...\sqrt{N/k}\rfloor}\rangle$ reaches the neighborhood of the point $(0,-1)$. Measuring $|\psi_{\lfloor 0.785...\sqrt{N/k}\rfloor}\rangle$ results in getting index of a marked item, with probability almost 1.

4.2   One Faulty Marked Item

Let us now consider the case with

- $N-k$ non-marked items,
- $k-1$ marked items, and
- 1 *faulty* marked item.

To simplify the analysis we shall interpret the step of the algorithm as consequent application of three operators: ordinary diffusion D and ordinary query Q, and – with probability ϵ – error E, which negates back the amplitude of the faulty marked item.

As the operation E is probabilistic one must deal not with a pure state $|\psi_t\rangle$, but with a mixed state ρ_t (probabilistic mixture of pure states). We shall denote components of the mixture after t steps as $|\psi_t^w\rangle$, where $w \in \{0,1\}^t$ stands for the sequence of t events: 0 – the query has negated the amplitude of the faulty marked item (DQ), and 1 – the query has left that amplitude of the faulty marked item unchanged (DQE). So the mixture ρ_t looks as follows:

$$\rho_t = \sum_{w \in \{0,1\}^t} \epsilon^{|w|} (1-\epsilon)^{t-|w|} |\psi_t^w\rangle\langle\psi_t^w|.$$

Transformations D, Q and E are symmetric w.r.t. permutations of amplitudes of non-faulty marked items, as well as permutation of amplitudes of non-marked items. So, in any state $|\psi_t^w\rangle$ of the mixture $|\psi_t^*\rangle$, amplitudes of all non-faulty marked items are equal to each other and amplitudes of all non-marked items are equal to each other. Thus, we can represent $|\psi_t^w\rangle$ as:

$$|\psi_t^w\rangle = \sum_{i \in U} \alpha_t^w |i\rangle + \sum_{\substack{j \in M, \\ j \neq i_k}} \beta_t^w |j\rangle + \gamma_t^w |i_k\rangle, \tag{5}$$

where U stands for the set of indexes of non-marked items and M stands for the set of indexes of k marked items. α_t^w, β_t^w and γ_t^w denote the amplitudes of respectively a non-marked item, a non-faulty marked item and the faulty marked item.

At each step of the algorithm for each of 2^t scenarios w we shall take care of three numbers:

$$\alpha_t^w \sqrt{N-k}, \qquad \beta_t^w \sqrt{k-1} \qquad \text{and} \qquad \gamma_t^w. \tag{6}$$

Since $|\psi_t^w\rangle$ are unit vectors we have

$$\sum_{i \in U} (\alpha_t^w)^2 + \sum_{\substack{j \in M, \\ j \neq f}} (\beta_t^w)^2 + (\gamma_t^w)^2 = 1.$$

Thus, values (6) meet the equality $\left(\alpha_t^w \sqrt{N-k}\right)^2 + \left(\beta_t^w \sqrt{k-1}\right)^2 + (\gamma_t^w)^2 = 1$ and correspond to a points on the unit sphere.

Initially the mixture consists of state $|\psi_0\rangle$ with amplitudes of all items being equal, so $\alpha = \beta = \gamma = \frac{1}{\sqrt{N}}$, and the numbers (6) for $t = 0$ are

$$\alpha_0 \sqrt{N-k} = \frac{\sqrt{N-k}}{\sqrt{N}}, \qquad \beta_0 \sqrt{k} = \frac{\sqrt{k-1}}{\sqrt{N}} \qquad \text{and} \qquad \gamma_0 = \frac{1}{\sqrt{N}}. \tag{7}$$

During the first step of the algorithm

- D does not change amplitudes of the state $|\psi_0\rangle$;
- Q negates the amplitudes of all marked items: $\beta_1^w = \gamma_1^0 = -\frac{1}{\sqrt{N}}$;
- E negates back the amplitude of the faulty marked item: $\gamma_1^1 = -\gamma_1^0 = \frac{1}{\sqrt{N}}$.

So the numbers (6) for $t = 1$ are as follows:

$$\begin{array}{llll}
\alpha_1^0 \sqrt{N-k} = \frac{\sqrt{N-k}}{\sqrt{N}}, & \beta_1^0 \sqrt{k-1} = -\frac{\sqrt{k-1}}{\sqrt{N}}, & \gamma_1^0 = -\frac{1}{\sqrt{N}} & \text{for } w = 0; \\
\alpha_1^1 \sqrt{N-k} = \frac{\sqrt{N-k}}{\sqrt{N}}, & \beta_1^1 \sqrt{k-1} = -\frac{\sqrt{k-1}}{\sqrt{N}}, & \gamma_1^1 = \frac{1}{\sqrt{N}} & \text{for } w = 1.
\end{array} \tag{8}$$

According to (7) and (8), transformation $|\psi_0\rangle\langle\psi_0| \xrightarrow{DQ(E)} (1-\epsilon)|\psi_1^0\rangle\langle\psi_1^0| + \epsilon|\psi_1^1\rangle\langle\psi_1^1|$ can be represented on the unit sphere as shown on Figure 3.
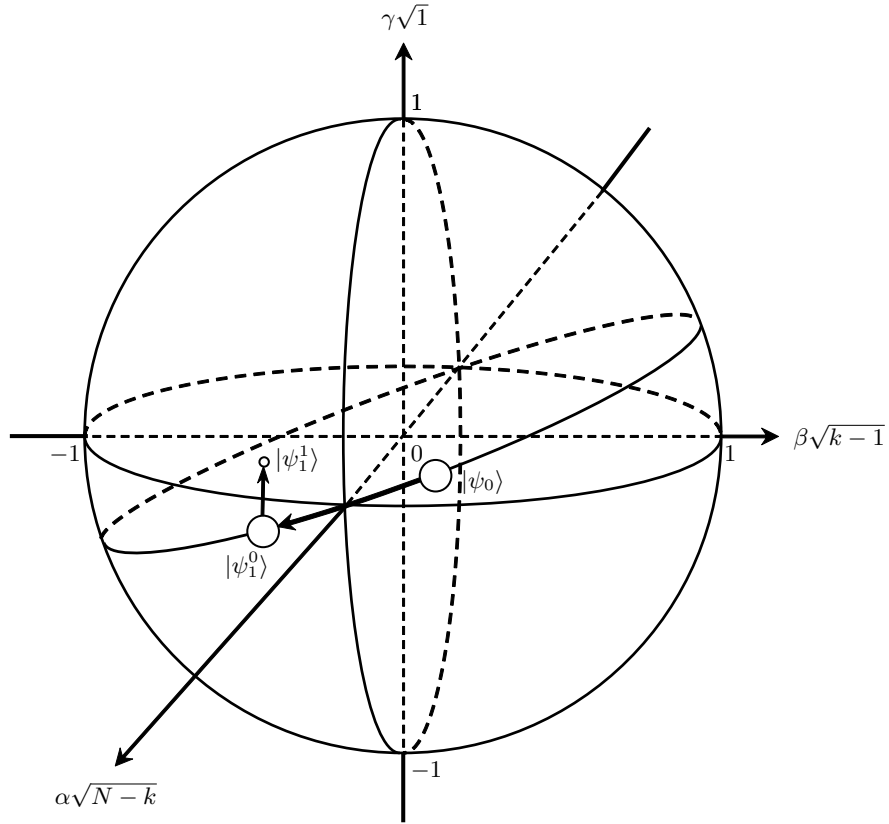
Fig. 3. The first step of Grover's algorithm with a faulty marked item. Size of a ball corresponds to a probability of the state in the mixture. $|\psi_0^*\rangle\langle\psi_0^*| = 1|\psi_0\rangle$ and $|\psi_1^*\rangle\langle\psi_1^*| = (1 - \epsilon)|\psi_1^0\rangle\langle\psi_1^0| + \epsilon|\psi_1^1\rangle\langle\psi_1^1|$

Note that if $\epsilon = 0$ the state of the algorithm travels clockwise along the slanted orthodrome[3] which contains points $|\psi_0\rangle$ and $(1,0,0)$. The travel lasts until the state reaches the neighborhood of the vertical orthodrome (hereafter we call it *meridian*) where $\alpha = 0$ after $t \approx 0.785\ldots\sqrt{N/k}$ steps.
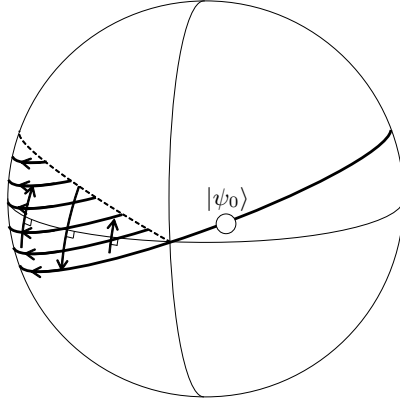

Fig. 4. Probable routes of the initial state $|\psi_0\rangle$ in the run of Grover's algorithm with a faulty marked item.

If $k \ll N$ the rotation angle (4) is sufficiently small. The run of the algorithm can be viewed as clockwise rotation of a state in parallel to the slanted orthodrome (DQ-movement) with occasional (ϵ-probable) up-and-down jumps around the horizontal orthodrome (hereafter we call it *equator*), which correspond to operator E, as shown on Figure 4. During the first $0.785\ldots\sqrt{N/k}$ steps, the state cannot go out of the area which is covered with arrows on the figure.

As we already mentioned, $0.785\ldots\sqrt{N/k}$ steps are necessary to reach the desired plane where $\alpha = 0$, given that no fault occurs on the way (in our notation: in expression (5), $\alpha^{00\ldots0}_{\lfloor 0.785\ldots\sqrt{N/k}\rfloor} \approx 0$).

But what could the length of the route be if some faults occur on the state's way to the desired plane? In the two following subsections we will derive upper bounds for the effect of these faults.

At most one fault First, let us assume that the total number of faults is at most one. Although this assumption seems to be rather implausible, we have some arguments for it:

---

[3] Orthodrome, also known as a great circle, of a sphere is the intersection of the sphere with a plane which passes through the center point of the sphere.

○ for sufficiently small ϵ, we have $\ldots \ll \epsilon^3 \ll \epsilon^2 \ll \epsilon$, so that probability of more than one fault $\sum_{f=2}^{t} \binom{t}{f} \epsilon^f (1-\epsilon)^{t-f} < t^2 \epsilon^2$ could be neglected for number of steps $t \in o\left(\frac{1}{\epsilon}\right)$;

○ as we shall see later, the second and all subsequent faults have smaller effect and even have great chances to drive the state closer to the desired meridian.
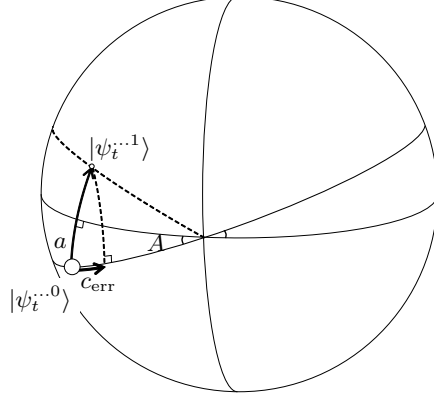

Fig. 5. Metrics for a fault.

Let us calculate the effect of a fault in the sense of its projection onto the "no-faults" route. On the Figure 5 we illustrate ϵ-probable transformation $|\psi_i^{\cdots 0}\rangle \xrightarrow{E} |\psi_i^{\cdots 1}\rangle$, which happened on some step t. The fault increases the angular distance to the desired meridian ($\alpha = 0$) by c_{err}. Using rules of spherical trigonometry ((R8) and (R7)) we have:

$$c_{\mathrm{err}} = \arctan\left(\tan 2a \ \cos\arcsin\frac{\cos A}{\cos a}\right) = \arctan\left(\tan 2a \ \sqrt{1 - \frac{\cos^2 A}{\cos^2 a}}\right), \quad (9)$$

where $A = \arctan\frac{1}{\sqrt{k-1}}$ is angle between the two equators, and a is the distance between $|\psi_i^{\cdots 0}\rangle$ and the horizontal equator. Note that a is at most A ($a = A$ only when $|\psi_t^w\rangle$ reaches the desired meridian), so $1 - \frac{\cos^2 A}{\cos^2 a} \geq 0$.

In equation (9) we assumed that $|\psi_i^{\cdots 0}\rangle$ is located on the bottom-margin of the arrow-filled area of the Figure 4 (which always holds for one fault case). For $|\psi_i^{\cdots 0}\rangle$ located above the bottom margin, we should calculate (9) for a smaller value of A, which will result in smaller value of c_{err}. For $|\psi_i^{\cdots 0}\rangle$ located above the horizontal equator, the fault-effect c_{err} is negative, i.e. the resulting state $|\psi_i^{\cdots 1}\rangle$ is closer to the desired meridian w.r.t. the direction in parallel to the slanted orthodrome. Relaxing the above-mentioned assumption, we can conclude the following rough bound:

$$c_{\text{err}} \leq \arctan\left(\tan 2a \sqrt{1 - \frac{\cos^2 A}{\cos^2 a}}\right). \tag{10}$$

Now, based on the inequality (10) we shall derive more precise bounds.

If the number of non-faulty marked items $k - 1 \geq 1$, then the angle $A = \arctan\frac{1}{\sqrt{k-1}} \in \left(\arctan\frac{1}{\infty}; \arctan\frac{1}{1}\right] = \left(0; \frac{\pi}{4}\right]$. So we have $0 \leq a \leq A \leq \frac{\pi}{4}$.

Now let us consider different values of a. If $0 \leq a \leq \frac{\pi}{6}$, then (9) is bounded by

$$c_{\text{err}} \leq \max_{\substack{0 \leq a \leq A, \\ a \leq \frac{\pi}{6}}} \arctan\left(\tan 2a \sqrt{1 - \frac{\cos^2 A}{\cos^2 a}}\right) \leq \frac{\pi}{4}, \tag{11}$$

where the inequalities become equalities for $A = \frac{\pi}{4}$ and $a = \frac{\pi}{6}$.

If $\frac{\pi}{6} < a \leq \frac{\pi}{4}$, then we can follow that the state $|\psi_i^{\cdots 0}\rangle$ is gone far away from the point "$\alpha\sqrt{N-k} = 1$" of the unit sphere. This distance between the point $(1, 0, 0)$ and the state $|\psi_i^{\cdots 0}\rangle$ can be derived from the rule (R2):

$$c = \arcsin\frac{\sin a}{\sin A} \geq \arcsin\frac{\sin \pi/6}{\sin \pi/4} = \frac{\pi}{4} \tag{12}$$

Since the total distance between the point "$\alpha\sqrt{N-k} = 1$" and any point of the meridian "$\alpha\sqrt{N-k} = 0$" is exactly $\frac{\pi}{2}$, we follow that the state $|\psi_i^{\cdots 0}\rangle$ is at most $\frac{\pi}{2} - \frac{\pi}{4} = \frac{\pi}{4}$ far from the desired meridian.

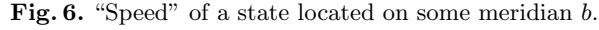From (11) and (12) we formulate the following joint conclusion:

Corollary 1. *At least one of the following claims holds for any state $|\psi_i^{\cdots 0}\rangle$ with $0 \leq a \leq A \leq \frac{\pi}{4}$:*

- *either the fault-effect $c_{\text{err}} \leq \frac{\pi}{4}$,*
- *or the state $|\psi_i^{\cdots 0}\rangle$ is already at most $\frac{\pi}{4}$ far from the desired meridian "$\alpha = 0$".*

Any number of faults Now let us use another approach to study the evolution of a state in the considered settings. Transformation $|\psi_t^w\rangle \xrightarrow{DQ} |\psi_{t+1}^{w,0}\rangle$ drives the state $|\psi_t^w\rangle$ clockwise in parallel to the slanted orthodrome by a distance, which depends on the position of this state on the unit sphere.

On Figure 6 we show a "speed" for each possible position of the state $|\psi_t^w\rangle$. On the "no-faults" route (i.e. the slanted orthodrome) the speed coincides with that of the original Grover's algorithm: $v_G = 2\arcsin\frac{\sqrt{k}}{\sqrt{N}} \approx 2\sqrt{\frac{k}{N}}$. After a state jumps up, its speed decreases depending on its distance to the slanted orthodrome: e.g. on the parallel circle which contains point "$\beta\sqrt{k-1} = 1$" of the units sphere, its speed is $v_G \cos A$.

We can also calculate the speed of a state w.r.t. the direction in parallel to the horizontal equator, i.e. the speed of its projection onto the horizontal equator v_{Π}.

Fig. 6. "Speed" of a state located on some meridian b.

Obviously, among all states on some meridian b, the uppermost state $|\psi_b^\uparrow\rangle$ has the least speed. Distance between $|\psi_b^\uparrow\rangle$ and the point "$\alpha\sqrt{N}=1$" of the unit sphere, can be derived from angle A, distance b and rule (R6): $c = \arctan\frac{\tan b}{\cos A}$. Distance between $|\psi_b^\uparrow\rangle$ and the slanted orthodrome can be derived from distance c, angle $2A$ and rule (R2): $a' = \arcsin\left(\sin 2A \sin c\right) = \arcsin\left(\sin 2A \sin\arctan\frac{\tan b}{\cos A}\right)$. And the speed of $|\psi_b^\uparrow\rangle$

$$v^\uparrow(b) = v_G \cos(a') = v_G\sqrt{1 - \frac{\sin^2 2A\ \tan^2 b}{\cos^2 A + \tan^2 b}}$$

serves as a natural lower bound for the speed of any state located on the same meridian b:

$$v(b) \geq v^\uparrow(b) = v_G\sqrt{1 - \frac{\sin^2 2A\ \tan^2 b}{\cos^2 A + \tan^2 b}}.$$

Projection of the speed $v(b)$ onto the horizontal equator might be slightly less:

$$v_\Pi(b) \geq v(b)\cos A \geq v_G\sqrt{1 - \frac{\sin^2 2A\ \tan^2 b}{\cos^2 A + \tan^2 b}}\cos A. \tag{13}$$

Vertical jumps leave states on the same meridians, so faults does not affect value b. Moving at least at speed (13), a state will pass distance $\frac{\pi}{2}$ in at most $\int_0^{\frac{\pi}{2}} \frac{1}{v_\Pi(b)}\,\mathrm{d}b$ steps. From (13) we obtain an upper bound for the number of steps until some meridian b^* (for arbitrary number of faults, i.e. for any ϵ):

$$t_{b^*} \leq \int_0^{b^*} \frac{1}{v_\Pi(b)}\,\mathrm{d}b \leq \int_0^{b^*} \frac{1}{v_G\sqrt{1 - \frac{\sin^2 2A\ \tan^2 b}{\cos^2 A + \tan^2 b}}\cos A}\,\mathrm{d}b. \tag{14}$$

We note that on the fastest "no-fault" route a state will travel exactly at speed v_G, so that in the same many t_{b^*} steps it can reach at most $(v_G t_{b^*})^{\text{th}}$ meridian.

From (14) we can derive the upper bound for the distance between the two meridians b^* and $v_G t_{b^*}$:

$$v_G t_{b^*} - b^* \leq \cancel{v_G} \int_0^{b^*} \frac{1}{\cancel{v_G}\sqrt{1 - \frac{\sin^2 2A \ \tan^2 b}{\cos^2 A + \tan^2 b} \cos A}} \, \mathrm{d}b - b^* \tag{15}$$

For example, if we fix $b^* = \frac{3}{8}\pi$, then for any $0 \leq A \leq 0.1953\ldots\pi$, value (15) does not exceed $\frac{\pi}{4}$. That is, when the fastest state of a quantum ensemble reaches meridian $b^* + \frac{\pi}{4} = \frac{5}{8}\pi$, the slowest state of the ensemble with certainty reaches at least meridian $b^* = \frac{3}{8}\pi$.

4.3   Proof of theorem 1

We run standard Grover's algorithm $\frac{5}{4}$ times longer than usually, and then perform a measurement.

- If at most one fault is promised, and $A \leq 0.25\pi$,[4] then we use Corollary 1 and follow that any component of the resulting mixture $|\psi^*\rangle$ is at most $\frac{\pi}{8}$ far from the meridian "$\alpha = 0$".
- If $A \leq 0.1953\ldots\pi$,[5] then we substitute $b^* = \frac{3}{8}\pi$ in (15) and follow exactly the same.

Measurement of such $|\psi^*\rangle$ results in finding a marked item (the faulty or a non-faulty one) with probability at least $\cos^2 \frac{\pi}{8} = 0.853553\ldots$

- Otherwise, if $0.1953\ldots\pi < A \leq 0.25\pi$ and there is no promise on the number of faults, it means that there is exactly 1 non-faulty marked element (so $A = 0.25\pi$).

In this specific case we run standard Grover's algorithm ≈ 1.34 times longer than usually, and then perform a measurement. We substitute $A = 0.25\pi, b^* \approx 0.33\pi$ in (15) and follow that value (15) does not exceed $\approx 0.34\pi$. That is, when the fastest state of a quantum ensemble reaches meridian $b^* + 0.34\pi = 0.67\pi(= 0.5 \times 1.34\pi)$, the slowest state of the ensemble with certainty reaches at least meridian $b^* = 0.33\pi$. Measurement of such $|\psi^*\rangle$ results in finding a marked item (the faulty or a non-faulty one) with probability at least $\cos^2 0.17\pi = 0.74\ldots$.

$\square$

---

[4] $A \leq 0.25\pi$ means that there is at least as many non-faulty marked items as faulty marked items. Since we limit our considerations with only one faulty marked item, it suffices with only one non-faulty marked item.

[5] For one faulty marked item, it means existence of at least $\lceil \mathrm{arccot}\, 0.1953\ldots\pi \rceil = \lceil 1.02047 \rceil = 2$ non-faulty marked items

5   Limiting behavior

In this section we analyze the state of the algorithm after a large number of steps. We consider a density matrix of the state and describe how transformations of the algorithm change the state. We prove an existence of the limiting state and give probabilities of finding a non-faulty marked, as well as faulty marked item then measuring the state.

Proof of theorem 2

Consider the density matrix ρ_t of the quantum state of Grover's algorithm after t queries. Due to symmetry, we can assume that the first k basis states correspond to the marked elements. Note that Grover's algorithm acts in the same way on all non-faulty marked elements, as well as on all non-marked elements. Therefore, the state of the algorithm is a probabilistic mixture of pure states of the form

$$\alpha|\psi_+\rangle + \beta|i_k\rangle + \gamma|\psi_-\rangle. \tag{16}$$

The density matrix ρ_t, then, takes the form

$$\rho_t = \begin{bmatrix} a & \dots & a & a' & c & \dots & c \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a & \dots & a & a' & c & \dots & c \\ a' & \dots & a' & b & d' & \dots & d' \\ c & \dots & c & d' & d & \dots & d \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ c & \dots & c & d' & d & \dots & d \end{bmatrix} \tag{17}$$

because the density matrix for every pure state (16) in the mixture ρ_t is of this form.

Next we consider the effect of the faulty query Q' and the diffusion transformation D on the density matrix ρ.

Lemma 1 *The effect of the faulty query Q' on the density matrix ρ_t is:*

$$\begin{aligned} a &\mapsto a \\ a' &\mapsto -(2p-1)a' \\ b &\mapsto b \\ c &\mapsto -c \\ d' &\mapsto (2p-1)d' \\ d &\mapsto d \end{aligned} \tag{18}$$

Proof. Follows from [AB+13, formula (2)].

Lemma 2 *The effect of the diffusion transformation D on the density matrix ρ is:*

$$\rho_{i,j} \mapsto 4V - 2V_{i,\cdot} - 2V_{\cdot,j} + \rho_{i,j}, \tag{19}$$

where $V = \frac{1}{N^2} \sum_{i,j} \rho_{i,j}$ is the average of all elements of ρ, $V_{i,\cdot} = \frac{1}{N} \sum_j \rho_{i,j}$ is the average of ith row and $V_{\cdot,j} = \frac{1}{N} \sum_i \rho_{i,j}$ is the average of jth column of ρ.

Proof. First we right multiply $\rho = (\rho_{i,j})$ by

$$D = \begin{bmatrix} -1 + \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & -1 + \frac{2}{N} & \cdots & \frac{2}{N} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & -1 + \frac{2}{N} \end{bmatrix}.$$

We get matrix $\rho' = \rho D$ where

$$\rho'_{i,j} = \sum_k \rho_{i,k} \frac{2}{N} - \rho_{i,j} = 2V_{i,\cdot} - \rho_{i,j}. \tag{20}$$

Next we left multiply (20) by D and get matrix $\rho'' = D\rho D$ where

$$\rho''_{i,j} = \sum_k \frac{2}{N} (2V_{k,\cdot} - \rho_{k,j}) - (2V_{i,\cdot} - \rho_{i,j}) =$$

$$= \frac{4}{N} \sum_k V_{k,\cdot} - \frac{2}{N} \sum_k \rho_{k,j} - 2V_{i,\cdot} + \rho_{i,j} =$$

$$4V - 2V_{i,\cdot} - 2V_{\cdot,j} + \rho_{i,j}.$$

As $V_{i,\cdot} = V_{\cdot,i}$ (this follows from the structure of the density matrix ρ_t) we can use V_i to denote both $V_{i,\cdot}$ and $V_{\cdot,i}$.

Using the same argument as in [AB+13] we can prove $\lim_{t\to\infty} a' = 0$ and $\lim_{t\to\infty} d' = 0$. Consider t' such that for all $t > t'$ inequalities $a' < \epsilon$ and $d' < \epsilon$ hold. We will prove that at this moment all elements of ρ_t should be $O(\epsilon)$ close to their final values. The proof is done in two steps. First we prove that all V_i can differ by at most $O(\epsilon)$. Next, as a consequence, we derive $\Delta\rho_{i,j} = O(\epsilon)$.

Claim 1 $\forall i, j : V_i - V_j = O(\epsilon)$.

Proof. First, note that $V_1 = \ldots = V_{k-1}$ and $V_{N-k} = \ldots = V_N$. This follows from the structure of ρ_t.

Next, consider effect of D on elements $\rho_{1,k}$ and $\rho_{k,N}$. Both elements are $O(\epsilon)$. Corresponding changes $\Delta\rho_{1,k} = 4V - 2V_1 - 2V_k$ and $\Delta\rho_{k,N} = 4V - 2V_k - 2V_N$ should also be $O(\epsilon)$. Thus,

$$\Delta\rho_{1,k} - \Delta\rho_{k,N} = 2V_1 - 2V_N = O(\epsilon) \tag{21}$$

from which follows $V_1 - V_N = O(\epsilon)$.

Now consider $\Delta\rho_{1,k} = 4V - 2V_1 - 2V_k = O(\epsilon)$. By using (21) we can write

$$V = \frac{1}{N}((k-1)V_1 + V_k + (N-k)V_N) = \frac{1}{N}((N-1)V_1 + V_k + O(\epsilon)).$$

Putting this into $\Delta\rho_{1,k}$ and opening brackets we get

$$\frac{2N-4}{N}V_1 - \frac{2N-4}{N}V_k = O(\epsilon)$$

from which follows $V_1 - V_k = O(\epsilon)$.

Corollary 2. D *changes elements of* ρ_t *by at most* $O(\epsilon)$.

Proof. The change of element $\rho_{i,j}$ is equal to $\Delta\rho_{i,j} = 4V - 2V_i - 2V_j$. Using claim 1 we can rewrite this equation as

$$\Delta\rho_{i,j} = \frac{4}{N}(NV_i + O(\epsilon)) - 4V_i + O(\epsilon) = O(\epsilon).$$

Corollary 3. $c = O(\epsilon)$.

Proof. Consider the effect of Q' on $V_1 = (k-1)a + (N-k)c + O(\epsilon)$. Q' leaves a unchanged, but changes the sign of c. As the claim 1 should hold for all subsequent steps, Q' can not change value of V_1 by more than $O(\epsilon)$. Thus, $V_1(c) - V_1(-c)$ should be $O(\epsilon)$, which means that $c = O(\epsilon)$.

Corollary 4. Q' *changes elements of* ρ_t *by at most* $O(\epsilon)$.

Proof. Trivially follows from (18) and the previous corollary.

We can chose ϵ to be arbitrary small, thus, we have

$$\rho_{lim} = \begin{bmatrix} a & \dots & a & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a & \dots & a & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & b & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & d & \dots & d \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & d & \dots & d \end{bmatrix}.$$

As $(k-1)a = b = (N-k)d$ (follows from $V_1 = V_k = V_N$) and $(k-1)a + b + (N-k)d = 1$ (property of density matrix) we have $(k-1)a = b = (N-k)d = \frac{1}{3}$ which completes the proof of the theorem.

$\square$

6 Summary and open problems

In this paper we focus on the case where search space contains multiple non-faulty and one faulty marked element.

First we show that if there are at least two non-faulty marked elements or it there is at most one fault, then it is still possible to find a non-faulty marked element in $O(\sqrt{N})$ queries with $\Theta(1)$ probability.

Second, we analyze the limiting behavior of the algorithm for a large number of steps and show the existence and structure of limiting state ρ_{lim}.

It is an open question to generalize the results for more than one faulty marked element. Although the generalization of Theorem 2 seems to be straightforward it is not given here. The generalization of Theorem 1 might be tricky as one needs to deal with hyper-spherical geometry. One simple case, in which the theorem still holds for multiple faulty marked elements, is synchronized-fault-case, where each query either fails or succeeds on all faulty marked elements.

References

Amb04.   A. Ambainis. Quantum search algorithms. *SIGACT News*, 35(2):22-35, 2004.

AB+13.   A. Ambainis, A. Backurs, N. Nahimovs, A. Rivosh. Grover's algorithm with errors. *Proceedings of MEMICS 2012*, LNCS 7721:180-189, 2013.

Gro96.   L. Grover. A fast quantum mechanical algorithm for database search. *Proceedings of the 28th ACM STOC*, 212-219, 1996.

HJ06.   R. Horn, C. Johnson. *Matrix Analysis*, Cambridge University Press, 2006.

KLM07.   P. Kaye, R. Laflamme, M. Mosca. *An Introduction to Quantum Computing*, Cambridge University Press, 2007.

RS08.   O. Regev, L. Schiff. Impossibility of a Quantum Speed-up with a Faulty Oracle *Proceedings of ICALP'2008*, LNCS 5125:773-781, 2008.

Tod86.   I. Todhunter. Spherical Trigonometry (5th ed.). *MacMillan*, 1886.